

日本国特許庁  
JAPAN PATENT OFFICE

別紙添付の書類に記載されている事項は下記の出願書類に記載されている事項と同一であることを証明する。

This is to certify that the annexed is a true copy of the following application as filed with this Office.

出願年月日 Date of Application: 2002年11月15日

出願番号 Application Number: 特願2002-331677

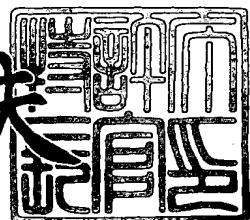
[ST. 10/C]: [JP2002-331677]

出願人 Applicant(s): ソニー株式会社

2003年 8月25日

特許庁長官  
Commissioner,  
Japan Patent Office

今井康夫



【書類名】 特許願

【整理番号】 0290507703

【提出日】 平成14年11月15日

【あて先】 特許庁長官殿

【国際特許分類】 G06F 15/31

【発明者】

【住所又は居所】 東京都品川区北品川6丁目7番35号 ソニー株式会社  
内

【氏名】 菅 真紀子

【特許出願人】

【識別番号】 000002185

【氏名又は名称】 ソニー株式会社

【代理人】

【識別番号】 100094053

【弁理士】

【氏名又は名称】 佐藤 隆久

【手数料の表示】

【予納台帳番号】 014890

【納付金額】 21,000円

【提出物件の目録】

【物件名】 明細書 1

【物件名】 図面 1

【物件名】 要約書 1

【包括委任状番号】 9707389

【プルーフの要否】 要



【書類名】 明細書

【発明の名称】 回路構成方法、その装置およびそのプログラム

【特許請求の範囲】

【請求項 1】

所定のデータに対してそれぞれ異なる複数の第1の演算を施す演算回路の回路設計方法であって、

前記複数の第1の演算のそれぞれを構成する複数の第2の演算のうち、同じデータに対して同じ演算を行う前記第2の演算を特定する第1の工程と、

前記複数の第1の演算で共用され前記第1の工程で特定された前記第2の演算を行う第1の演算回路と、前記複数の第1の演算のそれぞれを構成する前記複数の第2の演算のうち前記第1の工程で特定された前記第2の演算以外の演算を行う第2の演算回路とからなる前記演算回路を構成する第2の工程とを有する回路構成方法。

【請求項 2】

前記第1の演算は、線形変換の演算であり、

前記第2の演算は、加算である

請求項1に記載の回路構成方法。

【請求項 3】

前記複数の第1の演算が、前記所定のデータに対して第1の線形変換をそれぞれ異なる所定の回数施す演算である場合に、

前記複数の第1の演算のそれぞれについて、前記所定の回数に対応する数の前記第1の線形変換を合成した第2の線形変換を規定する第3の工程をさらに有し、

前記第1の工程において、前記第3の工程で前記複数の第1の演算のそれぞれについて規定された前記第2の線形変換を構成する前記複数の第2の演算のうち、同じデータに対して同じ演算を行う前記第2の演算を特定する

請求項1に記載の回路構成方法。

【請求項 4】

前記第2の工程において、前記第3の工程で規定された前記第2の線形変換を

基に、前記所定のデータに対して前記複数の第1の演算を並列に行うように前記演算回路を構成する

請求項3に記載の回路構成方法。

【請求項5】

前記所定データは、所定の線形空間上の所定の基底により、ベクトルで表現されたものであり、

前記線形変換は、前記線形空間上で規定された変換である

請求項3に記載の回路構成方法。

【請求項6】

前記所定の線形空間を下記(1-1)で示し、前記所定の基底として下記(1-2)に示す基底を用い、下記(1-2)に示す基底を基に前記所定のデータであるデータaが下記(1-3)のように示されるとき、当該データaをm次元ベクトルとして下記(1-4)で示し、前記第1の線形変換を下記(1-1)に示す線形空間上の線形変換Dとし、前記複数の演算の結果であるデータbをk次元ベクトルとして下記(1-5)で示し、下記(1-5)に示すデータbを構成する各演算の結果を示すデータb<sub>i</sub>をd<sub>i</sub>次元ベクトルとして下記(1-6)で示した場合に

前記第3の工程において、d<sub>i</sub>行m列の行列Dで構成され前記第2の線形変換を行う下記(1-7)で示される行列Mを規定し、

前記第1の工程において、前記第3の工程で規定された下記(1-7)を基に、前記複数の第2の演算のうち、同じデータに対して同じ演算を行う前記第2の演算を特定する

請求項3に記載の回路構成方法。

ここで、m, d<sub>i</sub>は2以上の整数であり、前記複数の演算の少なくとも一つに対応する前記所定の回数が2以上であり、kは2以上の整数である。

【数1】

$$\text{線形空間 } \mathbf{F}_{g^m} \quad (1-1)$$

【数2】

$$\{ \gamma_1, \gamma_2, \dots, \gamma_m \} \quad (1-2)$$

【数3】

$$a = a_1 \gamma_1 + a_2 \gamma_2 + \cdots + a_m \gamma_m \quad (1-3)$$

【数4】

$$a = \begin{pmatrix} a_1 \\ a_2 \\ \vdots \\ \vdots \\ a_m \end{pmatrix} \quad (1-4)$$

【数5】

$$b = \begin{pmatrix} b_1 \\ b_2 \\ \vdots \\ \vdots \\ b_k \end{pmatrix} \quad (1-5)$$

【数6】

$$b_i = \begin{pmatrix} b_{i,1} \\ b_{i,2} \\ \vdots \\ \vdots \\ b_{i,d_i} \end{pmatrix} \quad (1-6)$$

【数7】

$$M = \begin{pmatrix} D \\ D^2 \\ \vdots \\ \vdots \\ D^k \end{pmatrix} \quad (1-7)$$

【請求項7】

前記所定の基底として下記(1-8)に示す基底を用い、前記データaが下記(1-9)のように示されるとき、前記データaをm次元ベクトルとして下記(1-10)の示す

請求項6に記載の回路構成方法。

【数8】

$$\{1, \gamma, \gamma^2, \cdots, \gamma^{m-1}\} \quad (1-8)$$



## 【数9】

$$a = a_0 + a_1 \gamma + a_2 \gamma^2 + a_3 \gamma^3 + \cdots + a_{m-1} \gamma^{m-1} \quad (1-9)$$

## 【数10】

$$a = \begin{pmatrix} a_0 \\ a_1 \\ a_2 \\ \vdots \\ \vdots \\ a_{m-1} \end{pmatrix} \quad (1-10)$$

## 【請求項8】

前記第3の工程において、前記線形空間上の元 $\gamma$ を基に $\gamma^r$ 倍の演算を行う前記行列Dで構成された前記行列Mを規定する

請求項6に記載の回路構成方法。

## 【請求項9】

所定のデータに対してそれぞれ異なる複数の第1の演算を施す演算回路の回路設計装置であって、

前記複数の第1の演算のそれぞれを構成する複数の第2の演算のうち、同じデータに対して同じ演算を行う前記第2の演算を特定する第1の手段と、

前記複数の第1の演算で共用され前記第1の手段で特定された前記第2の演算を行う第1の演算回路と、前記複数の第1の演算のそれぞれを構成する前記複数の第2の演算のうち前記第1の手段で特定された前記第2の演算以外の演算を行う第2の演算回路とからなる前記演算回路を構成する第2の手段と

を有する回路構成装置。

## 【請求項10】

所定のデータに対してそれぞれ異なる複数の第1の演算を施す演算回路の回路設計装置で実行されるプログラムであって、

前記複数の第1の演算のそれぞれを構成する複数の第2の演算のうち、同じデータに対して同じ演算を行う前記第2の演算を特定する第1の手順と、

前記複数の第1の演算で共用され前記第1の手順で特定された前記第2の演算を行う第1の演算回路と、前記複数の第1の演算のそれぞれを構成する前記複数

の第2の演算のうち前記第1の手順で特定された前記第2の演算以外の演算を行う第2の演算回路とからなる前記演算回路を構成する第2の手順とを有するプログラム。

#### 【発明の詳細な説明】

##### 【0001】

###### 【発明が属する技術分野】

本発明は、例えば、誤り訂正符号や復号などを行う場合に用いられる線形変換などの演算を行う演算回路の回路構成方法、その装置およびそのプログラムに関する。

##### 【0002】

###### 【従来の技術】

例えば、ハミング符号などの誤り訂正符号や復号では、有限体上で規定された線形空間で種々の線形変換の演算が行われる。

このような線形変換の演算は、例えば、線形空間上の所定の基底により、線形空間上の元をベクトルで表現し、このベクトルに対して線形変換の演算を施して新たなベクトルを得る。

上述した誤り訂正符号や復号では、例えば、複数ビットの所定データに対してそれぞれ異なる線形変換の複数の演算を行なう場合がある。

従来では、例えば、上記複数の演算をそれぞれ独立して行なうように演算回路を構成（設計）している。

##### 【0003】

###### 【発明が解決しようとする課題】

しかしながら、上述したように、上記複数の演算をそれぞれ独立して行なうよう演算回路を構成すると、演算回路が大規模になるという問題がある。

##### 【0004】

本発明は上述した従来技術の問題点に鑑みてなされ、所定データに対してそれぞれ異なる複数の演算を行なう演算回路を構成する場合に、当該演算回路を小規模に構成できる回路構成方法、その装置およびそのプログラムを提供することを目的とする。

## 【0005】

## 【課題を解決するための手段】

上述した従来技術の問題点を解決し、上述した目的を達成するために、第1の発明の回路設計方法は、所定のデータに対してそれぞれ異なる複数の第1の演算を施す演算回路の回路設計方法であって、前記複数の第1の演算のそれぞれを構成する複数の第2の演算のうち、同じデータに対して同じ演算を行う前記第2の演算を特定する第1の工程と、前記複数の第1の演算で共用され前記第1の工程で特定された前記第2の演算を行う第1の演算回路と、前記複数の第1の演算のそれぞれを構成する前記複数の第2の演算のうち前記第1の工程で特定された前記第2の演算以外の演算を行う第2の演算回路とからなる前記演算回路を構成する第2の工程とを有する。

## 【0006】

第1の発明の回路構成方法では、先ず、第1の工程において、複数の第1の演算のそれぞれを構成する複数の第2の演算のうち、同じデータに対して同じ演算を行う前記第2の演算が特定される。

そして、第2の工程において、前記複数の第1の演算で共用され前記第1の工程で特定された前記第2の演算を行う第1の演算回路と、前記複数の第1の演算のそれぞれを構成する前記複数の第2の演算のうち前記第1の工程で特定された前記第2の演算以外の演算を行う第2の演算回路とからなる前記演算回路が構成される。

## 【0007】

第2の発明の回路構成装置は、所定のデータに対してそれぞれ異なる複数の第1の演算を施す演算回路の回路設計装置であって、前記複数の第1の演算のそれぞれを構成する複数の第2の演算のうち、同じデータに対して同じ演算を行う前記第2の演算を特定する第1の手段と、前記複数の第1の演算で共用され前記第1の手段で特定された前記第2の演算を行う第1の演算回路と、前記複数の第1の演算のそれぞれを構成する前記複数の第2の演算のうち前記第1の手段で特定された前記第2の演算以外の演算を行う第2の演算回路とからなる前記演算回路を構成する第2の手段とを有する。

## 【0008】

第2の発明の回路構成装置では、第1の手段が、複数の第1の演算のそれぞれを構成する複数の第2の演算のうち、同じデータに対して同じ演算を行う前記第2の演算を特定する。

そして、第2の手段が、前記複数の第1の演算で共用され前記第1の手段で特定された前記第2の演算を行う第1の演算回路と、前記複数の第1の演算のそれぞれを構成する前記複数の第2の演算のうち前記第1の手段で特定された前記第2の演算以外の演算を行う第2の演算回路とからなる前記演算回路を構成する。

## 【0009】

第3の発明のプログラムは、所定のデータに対してそれぞれ異なる複数の第1の演算を施す演算回路の回路設計装置で実行されるプログラムであって、前記複数の第1の演算のそれぞれを構成する複数の第2の演算のうち、同じデータに対して同じ演算を行う前記第2の演算を特定する第1の手順と、前記複数の第1の演算で共用され前記第1の手順で特定された前記第2の演算を行う第1の演算回路と、前記複数の第1の演算のそれぞれを構成する前記複数の第2の演算のうち前記第1の手順で特定された前記第2の演算以外の演算を行う第2の演算回路とからなる前記演算回路を構成する第2の手順とを有する。

## 【0010】

## 【発明の実施の形態】

以下、本発明の実施形態について説明する。

## 〔本発明の関連技術〕

図1は、本発明の関連技術に係わる演算回路101の構成図である。

演算回路101は、データaを入力として、データb<sub>1</sub>～b<sub>k</sub>を出力する。

演算回路101は、iを1≤i≤kを満たす2以上の自然数、l<sub>i</sub>を自然数とした場合に、各系統で行列M<sub>i,1</sub>～M<sub>i,l<sub>i</sub></sub>によって規定された演算C<sub>i,1</sub>～C<sub>i,l<sub>i</sub></sub>を順に行う複数系統の演算回路モジュールを有し、これらの演算回路モジュールで並列に演算を行う。

各演算モジュールは、演算C<sub>i,1</sub>～C<sub>i,l<sub>i</sub></sub>をそれぞれ行う複数の演算回路2<sub>i,l<sub>j</sub></sub>を直接に接続して構成される。

演算回路101は、線形空間上の基底によりベクトル表現されたデータaを入力し、演算回路 $211_1 \sim 2k1_k$ でデータaに線形演算を施し、演算回路 $211_1 \sim 2k1_k$ からそれぞれ $b_1 \sim b_k$ を出力する。

#### 【0011】

図1に示す演算回路1は、各演算回路モジュール内の演算 $C_{i,1} \sim C_{i,l_i}$ を図2に示すように合成した演算回路モジュール $i1j$ （jは2以上の整数）を用いた演算回路201のように構成することで、小規模化および高速化が図れる。

この場合に、図2および下記(2-1)に示すように規定された線形変換列が、下記(2-2)に示すように合成される。

#### 【0012】

##### 【数11】

$$\begin{aligned} & \{C_{1,1}, C_{1,2}, \dots, C_{1,l_1}\}, \\ & \{C_{2,1}, C_{2,2}, \dots, C_{2,l_2}\}, \\ & \dots \dots \dots \dots \\ & \{C_{k,1}, C_{k,2}, \dots, C_{k,l_k}\}, \end{aligned} \tag{2-1}$$

$$\{C_{i,j-1}\text{の値域}\} \subset \{C_{i,j}\text{の定義域}\}$$

#### 【0013】

##### 【数12】

$$\begin{aligned} & C_{1,l_1} \circ \dots \circ C_{1,2} \circ C_{1,1} : a \mapsto b_1 \\ & C_{2,l_2} \circ \dots \circ C_{2,2} \circ C_{2,1} : a \mapsto b_2 \\ & \dots \\ & C_{k,l_k} \circ \dots \circ C_{k,2} \circ C_{k,1} : a \mapsto b_k \end{aligned} \tag{2-2}$$

#### 【0014】

このとき、上記(2-1)に示す演算 $C_{i,1} \sim C_{i,l_i}$ を線形変換を行う行列 $M_{i,1} \sim M_{i,l_i}$ とすると、上記(2-1), (2-2)は、それぞれ下記(2-3), (2-4)のように示される。

#### 【0015】

【数13】

$$\begin{aligned}
 & \{M_{1,1}, M_{1,2}, \dots, M_{1,l_1}\}, \\
 & \{M_{2,1}, M_{2,2}, \dots, M_{2,l_2}\}, \\
 & \dots \dots \dots \dots \\
 & \{M_{k,1}, M_{k,2}, \dots, M_{k,l_k}\},
 \end{aligned} \tag{2-3}$$

【0016】

【数14】

$$\begin{aligned}
 M_1 &:= M_{1,l_1}, \dots, M_{1,2}M_{1,1} : a \mapsto b_1 \\
 M_2 &:= M_{2,l_2}, \dots, M_{2,2}M_{2,1} : a \mapsto b_2 \\
 &\dots \\
 M_k &:= M_{k,l_k}, \dots, M_{k,2}M_{k,1} : a \mapsto b_k
 \end{aligned} \tag{2-4}$$

【0017】

これにより、演算回路201を、下記(2-5)に示す行列を行う回路として構成できる。

【0018】

【数15】

$$M := \begin{pmatrix} M_1 \\ M_2 \\ \dots \\ M_k \end{pmatrix} : a \mapsto \begin{pmatrix} b_1 \\ b_2 \\ \dots \\ b_k \end{pmatrix} \tag{2-5}$$

【0019】

次に、入力したデータF S 0に対して、第1の線形変換Dをそれぞれ異なる所定の回数施す複数の演算を行い、当該演算の結果であるデータ **$b_1 \sim b_k$** を出力する演算回路の構成方法について説明する。

図3は、このような演算回路301、並びにその周辺回路を説明するための図である。

【0020】

図3に示すように、セレクタ312において選択信号SELを基に、入力データaとデータMLSとのうち一方のデータが選択され、当該選択されたデータF S 0がレジスタ3130および演算回路301に出力される。

演算回路301は、セレクタ12から入力したデータFS0に対して、第1の線形変換Dをそれぞれ異なる所定の回数施す複数の演算を行い、当該演算の結果であるデータ $b_1 \sim b_k$ をそれぞれレジスタ $313_1 \sim 313_k$ に出力する。

レジスタ $313_0 \sim 313_k$ は、入力したデータFS0,  $b_1 \sim b_k$ を保持し、所定のタイミングで、これらをデータ $OUT_0 \sim OUT_k$ として出力する。

演算回路314は、データ $OUT_k$ を入力し、これに第1の線形演算Dを施して、その結果であるデータMSLをセレクタ312に出力する。

### 【0021】

演算回路301は、例えば、図3に示すように、それぞれ線形変換Dを行う複数の演算回路 $321_1 \sim 321_k$ を直列に接続し、データaを初段の回路 $321_1$ に入力し、個々の演算回路 $321_1 \sim 321_k$ で生成されたデータ $b_1 \sim b_k$ をレジスタ $313_1 \sim 313_k$ に出力するように構成（設計）される。

### 【0022】

ここで、図3に示す演算回路301は、有限体 $F(2^4)$ の元、 $\alpha, \alpha^2 + \alpha + 1 = 0$ に対して $\alpha$ 倍演算を行なうものである場合、図4に示すように構成される。

この場合に、図3に示すように、あるタイミングで入力されたデータaに対して、データ $OUT_0, OUT_1, OUT_2$ は、以下のようになる。

### 【0023】

#### 【表1】

$OUT_0 : a, a \times \alpha^{k+1}, a \times \alpha^{2k+2}, \dots,$

$OUT_1 : a \times \alpha, a \times \alpha^{k+2}, a \times \alpha^{2k+3}, \dots,$

$OUT_2 : a \times \alpha^2, a \times \alpha^{k+3}, a \times \alpha^{2k+4}, \dots,$

### 【0024】

ここで、 $FS0 = A_0 + A_1 \alpha$ とすると、以下のようになる。

$$FS0 \cdot \alpha = A_1 + (A_0 + A_1) \alpha$$

$$FS0 \cdot \alpha^2 = (A_0 + A_1) + A_0 \alpha$$

### 【0025】

従って、図4に示す演算回路 $321_1, 321_2$ は、図5に示すように、それ

ぞれ1個の加算回路351<sub>1</sub>，351<sub>2</sub>によって構成される。

### 【0026】

しかしながら、上述したように、演算回路301を設計すると、回路規模が大きくなるという問題がある。

また、演算回路301において、データaを初段の回路321<sub>1</sub>に入力してから最終段の回路321<sub>k</sub>からデータb<sub>k</sub>が出力されるまでの時間が長くなり、高性能な演算回路301を設計できないという問題がある。

### 【0027】

以下、上述した関連技術の問題点を解決する本発明の実施形態を説明する。

#### 〔第1実施形態〕

図6は、本実施形態の回路構成方法で構成（設計）される演算回路11の周辺回路を説明するための図である。

図6に示すように、セレクタ12において選択信号SELを基に、入力データaとデータMLSとのうち一方のデータが選択され、当該選択されたデータFS0がレジスタ130および演算回路11に出力される。

演算回路11は、セレクタ12から入力したデータFS0に対して、第1の線形変換Dをそれぞれ異なる所定の回数施す複数の演算を行い、当該演算の結果であるデータb<sub>1</sub>～b<sub>k</sub>をそれぞれレジスタ131～13<sub>k</sub>に出力する。

レジスタ130～13<sub>k</sub>は、入力したデータFS0，b<sub>1</sub>～b<sub>k</sub>を保持し、所定のタイミングで、これらをデータOUT<sub>0</sub>～OUT<sub>k</sub>として出力する。

演算回路14は、データOUT<sub>k</sub>を入力し、これに第1の線形演算Dを施して、その結果であるデータMSLをセレクタ12に出力する。

### 【0028】

本実施形態の回路構成方法は、図6に示す演算回路11を構成（設計）するものである。

### 【0029】

本実施形態では、所定の線形空間が、qを素数とした場合に有限体F<sub>q</sub>のm次拡大であり、その元がF<sub>q</sub>上のm次ベクトルで表現された場合に、当該所定の線形空間を下記（3-1）、あるいはF<sub>(q<sup>m</sup>)</sub>で示す。

【0030】

【数16】

線形空間  $F_{g^m}$ 

(3-1)

【0031】

また、所定の基底として下記 (3-2) に示す基底を用い、下記 (3-2) に示す基底を基に前記所定のデータであるデータ  $a$  を下記 (3-3) のように示す。

【0032】

【数17】

 $\{\gamma_1, \gamma_2, \dots, \gamma_m\}$ 

(3-2)

【0033】

【数18】

 $a = a_1 \gamma_1 + a_2 \gamma_2 + \dots + a_m \gamma_m$ 

(3-3)

【0034】

また、上記データ  $a$  を  $m$  次元ベクトルとして下記 (3-4) のように示す。

【0035】

【数19】

$$a = \begin{pmatrix} a_1 \\ a_2 \\ \vdots \\ a_m \end{pmatrix}$$

(3-4)

また、上記第1の線形変換  $D$  を上記 (3-1) に示す線形空間上の線形変換  $D$  とする。

【0036】

また、上記複数の演算の結果であるデータ  $b$  を  $k$  次元ベクトルとして下記 (3-5) で示し、下記 (3-5) に示すデータ  $b$  を構成する各演算の結果を示すデータ  $b_i$  を  $d_i$  次元ベクトルとして下記 (3-6) で示す。

ここで、 $m, d_i$  は 2 以上の整数であり、前記複数の演算の少なくとも一つに

対応する前記所定の回数が2以上であり、 $k$ は2以上の整数である。

【0037】

【数20】

$$\mathbf{b} = \begin{pmatrix} \mathbf{b}_1 \\ \mathbf{b}_2 \\ \vdots \\ \vdots \\ \mathbf{b}_k \end{pmatrix} \quad (3-5)$$

【0038】

【数21】

$$\mathbf{b}_i = \begin{pmatrix} \mathbf{b}_{i,1} \\ \mathbf{b}_{i,2} \\ \vdots \\ \vdots \\ \mathbf{b}_{i,d_i} \end{pmatrix} \quad (3-6)$$

【0039】

ここで、上記複数の演算を、それぞれ $OP_1 \sim OP_K$  とすると、これらは下記 (3-7) で示される。

【0040】

【数22】

$$\begin{array}{lll} OP_1 : \{D\}, & D : & a \mapsto b_1 \\ OP_2 : \{D, D\}, & D^2 := D \circ D : & a \mapsto b_2 \\ OP_3 : \{D, D, D\}, & D^3 := D \circ D \circ D : & a \mapsto b_3 \\ \dots \dots \dots \dots \dots & \dots & \dots \\ OP_k : \{D, D, D, \dots, D\}, & D^k := D \circ D \circ D \circ \dots \circ D : & a \mapsto b_k \end{array} \quad (3-7)$$

【0041】

そして、第1の線形変換 $D$ を表す $d \times m$ 列の行列を $M_d$ とすると、上記 (3-7) は、下記 (3-8) で示される。

【0042】

## 【数23】

$$\begin{array}{ll}
 \{M_d\}, & M_d : a \mapsto b_1 \\
 \{M_d, M_d\}, & M_d^2 : a \mapsto b_2 \\
 \{M_d, M_d, M_d\}, & M_d^3 : a \mapsto b_3 \quad (3-8) \\
 \cdots \cdots \cdots & \cdots \\
 \{M_d, M_d, M_d, \dots, M_d\}, & M_d^k : a \mapsto b_k
 \end{array}$$

## 【0043】

上記  $O P_1 \sim O P_K$  によって規定される変換列の合成を表した  $d \times m$  行列の行列  $M_d \sim M_d^k$  を縦に並べた  $k \times d \times m$  の行列  $M$  は、下記 (3-9) で示される。

## 【0044】

## 【数24】

$$M := \begin{pmatrix} M_d \\ M_d^2 \\ \cdots \\ M_d^k \end{pmatrix} : a \mapsto \begin{pmatrix} b_1 \\ b_2 \\ \cdots \\ b_k \end{pmatrix} = \begin{pmatrix} D \cdot a \\ D^2 \cdot a \\ \cdots \\ D^k \cdot a \end{pmatrix} \quad (3-9)$$

## 【0045】

上記 (3-9) に示すように、行列  $M$  が、データ  $a$  に対して第1の線形変換と、第2の変換  $D^2 \sim D^k$  をそれぞれ行う  $k$  個の演算を規定している。

## 【0046】

図7は、本実施形態の回路構成方法を実行するコンピュータ29を説明するための図である。

図7に示すように、コンピュータ29は、例えば、操作部31、ディスプレイ32、メモリ33およびCPU34を有し、これらがバス30を介して接続されている。

操作部31は、キーボードやマウスなどの操作手段であり、CPU34にプログラムの実行指示、データ選択指示、並びにデータ入力を行うために用いられる。

ディスプレイ32は、CPU34の処理結果を表示する。

メモリ33は、CPU34によって実行されるプログラム41と、プログラム

4 1 の実行に用いられるデータ 4 2 とを記憶する。

#### 【0047】

CPU34 は、プログラム 4 1 を実行して以下に示す処理を行い、プログラム 4 1 の実行過程でデータ 4 2 を用いて、演算回路 1 1 の回路を構成（設計）する処理を行う。

プログラム 4 1 は、本発明のプログラムに対応し、以下に示す各ステップの内容を示す手順を記述している。

また、CPU34 がプログラム 4 1 を実行することで、本発明の回路構成装置が構成され、CPU34 がステップ ST12 を実行して本発明の第 1 の手段を構成し、CPU34 がステップ ST13 を実行して本発明の第 2 の手段を構成する。

#### 【0048】

以下、本実施形態の回路構成方法の動作例を、CPU34 の処理と関連付けて説明する。

図 8 は、本実施形態の回路構成方法の動作例を説明するためのフローチャートである。

ステップ ST11：

CPU34 は、例えば、ユーザによる操作部 3 1 の操作に応じて、上記（3-4），（3-5），（3-6）に示すように演算回路 1 1 が行う演算の入力および出力の形式、並びに上記（3-7）に示すように演算回路 1 1 が行うそれぞれ所定の回数に対応する数の第 1 の線形変換 D をデータ a に施す複数の演算の内容を規定するデータを入力する。

#### 【0049】

ステップ ST12：

CPU34 が、ステップ ST11 で入力した上記（3-7）に示す演算回路 1 1 が行う複数の演算のそれぞれについて、上記所定の回数に対応する数の第 1 の線形変換 D を合成して得られる第 2 の線形変換（第 1 の演算）を行う上記（3-9）に示す行列 M を生成する処理を行う。

#### 【0050】

## ステップＳＴ13：

CPU34が、上記ステップＳＴ12で規定された複数の第2の線形変換（第1の演算）を構成する複数の第2の演算のうち、同じデータに対して同じ演算を行う前記第2の演算を特定する。

## 【0051】

## ステップＳＴ14：

CPU34が、複数の第2の線形演算（第1の演算）で共用されステップＳＴ13で特定された上記第2の演算を行う第1の演算回路と、上記複数の第1の演算のそれぞれを構成する上記複数の第2の演算のうちステップＳＴ13で特定された上記第2の演算以外の演算を行う第2の演算回路とからなる図9に示す演算回路11を構成する。

このとき、CPU34が、上記（3-9）に示すステップＳＴ12で生成された行列Mを基に、データFS0に対して第1の線形変換 $D \sim D^k$ をそれぞれ行うk個の演算を並列に行うように演算回路11の構成（設計）データを生成する。

具体的には、CPU34が、図9に示すように、データFS0に対して第1の線形変換 $D \sim D^k$ をそれぞれ行う演算回路 $21_1 \sim 21_k$ を並列に配置した演算回路11の構成を示す構成データを生成する。

## 【0052】

これにより、CPU34は、入力したデータFS0に上記（3-9）に示す行列Mで規定された線形変換を施し、データ $b_1 \sim b_k$ を出力するように構成された演算回路11の構成データを生成する。

## 【0053】

図9に示すように演算回路11を構成することで、レジスタ $13_0 \sim 13_k$ からの出力は、横方向を時間として、図10に示すようになる。

すなわち、演算回路1から、データ $b_1 \sim b_k$ が略同じタイミングで出力されるため、データOUT<sub>0</sub>～OUT<sub>K</sub>も略同じタイミングで出力される。

このとき、演算回路11が行う行列Mの演算と、演算回路11に入力されるデータFS0と、データOUT<sub>0</sub>～OUT<sub>K</sub>との関係は、下記（3-10）で示される。



## 【0054】

## 【数25】

$$M \cdot FSO = \begin{pmatrix} D \cdot FSO \\ D^2 \cdot FSO \\ D^3 \cdot FSO \\ \vdots \\ D^k \cdot FSO \end{pmatrix} = \begin{pmatrix} OUT_0 \\ OUT_1 \\ OUT_2 \\ \vdots \\ OUT_k \end{pmatrix} \quad (3-10)$$

## 【0055】

ここで、上記行列Mは上記（3-1）で規定された線形空間の元によって構成されるため、データ $OUT_1 \sim OUT_k$ （データ $b_1 \sim b_k$ ）は、上記線形空間の元とデータFSOの各要素との積、並びにそれらの和として規定される。そのため、それらの組み合わせは、高々有限となり、例えば、値kが値mに対して大きい場合に、図8に示すように、演算回路11から出力されたデータ $b_k$ を演算回路14およびセレクタ12を介して演算回路11にフィーロバックすることで、多様な演算に対応可能な演算回路11を小規模な構成で構築できる。

## 【0056】

以下、ここで、図9に示す演算回路11の演算回路 $21_1, 21_k$ は、有限体 $F(2^4)$ の元、 $\alpha, \alpha^2 + \alpha + 1 = 0$ に対して $\alpha$ 倍演算を行なうものである場合、図11に示す演算回路221のように構成される。

この場合に、図3に示すように、あるタイミングで入力されたデータaに対して、データ $OUT_0, OUT_1, OUT_2$ は、以下のようになる。

## 【0057】

$OUT_0 : a, a \times \alpha^{k+1}, a \times \alpha^{2k+2}, \dots,$

$OUT_1 : a \times \alpha, a \times \alpha^{k+2}, a \times \alpha^{2k+3}, \dots,$

$OUT_2 : a \times \alpha^2, a \times \alpha^{k+3}, a \times \alpha^{2k+4}, \dots,$

すなわち、 $FSO = A_0 + A_1 \alpha$ とすると、次のクロックサイクルにおけるデータ $OUT_0, OUT_1, OUT_2$ は、以下のようになる。

## 【0058】

OUT<sub>0</sub> : FS0 = A0 + A1  $\alpha$

OUT<sub>1</sub> : FS0  $\cdot$   $\alpha$  = A1 + (A0 + A1)  $\alpha$

OUT<sub>2</sub> : FS0  $\cdot$   $\alpha$   $\cdot$   $\alpha$  = (A0 + A1) + A0  $\alpha$

### 【0059】

この場合に、前述した図8に示すステップST13において、CPU34が、上記 $\alpha$ 倍演算を構成する複数の第2の演算のうち、同じデータに対して同じ演算を行う上記第2の演算、すなわち、演算「A0 + A1」を特定する。

そして、図8に示すステップST14において、CPU34が、複数の $\alpha$ 倍演算（すなわち、 $\alpha$ 倍演算と、 $\alpha^2$ 倍演算）で共用されステップST13で特定された演算「A0 + A1」を行う図11に示す第1の演算回路115（図11では加算回路）と、複数の $\alpha$ 倍演算のそれぞれを構成する上記複数の第2の演算のうちステップST13で特定された上記第2の演算以外の演算を行う第2の演算回路（図11に示す例では無し）とからなる図11に示す演算回路11aを構成する。

### 【0060】

なお、上述した実施形態において、上記第1の線形変換が、上記（3-1）で規定した線形空間の元 $\gamma$ に対して $\gamma^r$ 倍演算（ $\times \gamma^r$ ）を行うものである場合には、上記複数の演算を、それぞれOP<sub>1</sub>～OP<sub>K</sub>とすると、これらは下記（3-11）で示される。

### 【0061】

#### 【数26】

OP <sub>1</sub> :	$\{(\times \gamma^r)\},$	$(\times \gamma^r):$	$a \mapsto b_1$
OP <sub>2</sub> :	$\{(\times \gamma^r), (\times \gamma^r)\},$	$(\times \gamma^r) \circ (\times \gamma^r) :$	$a \mapsto b_2$
OP <sub>3</sub> :	$\{(\times \gamma^r), (\times \gamma^r), (\times \gamma^r)\},$	$(\times \gamma^r) \circ (\times \gamma^r) \circ (\times \gamma^r) :$	$a \mapsto b_3$
	...	...	...
OP <sub>K</sub> :	$\{(\times \gamma^r), (\times \gamma^r), (\times \gamma^r), \dots, (\times \gamma^r)\},$	$(\times \gamma^r) \circ (\times \gamma^r) \circ (\times \gamma^r) \circ \dots \circ (\times \gamma^r) \circ : a \mapsto b_K$	

(3-11)

### 【0062】

そして、第1の線形変換Dを表すd行m列の行列をMrとすると、上記（3-11）は、下記（3-12）で示される。

## 【0063】

## 【数27】

$$\begin{array}{ll}
 \{M_r\}, & M_r : a \mapsto b_1 \\
 \{M_r, M_r\}, & M_r^2 : a \mapsto b_2 \\
 \{M_r, M_r, M_r\}, & M_r^3 : a \mapsto b_3 \quad (3-12) \\
 \cdots \cdots \cdots & \cdots \\
 \{M_r, M_r, M_r, \dots, M_r\}, & M_r^k : a \mapsto b_k
 \end{array}$$

## 【0064】

上記OP<sub>1</sub>～OP<sub>K</sub>によって規定される変換列の合成を表したd行m列の行列M<sub>r</sub>～M<sub>r<sup>k</sup></sub>を縦に並べたk・d行×mの行列M<sub>r</sub>は、下記(3-13)で示される。

ここで、M<sub>r<sup>x</sup></sub>(xは1≤x≤kを満たす整数)は、X個のM<sub>r</sub>を合成した行列である。

## 【0065】

## 【数28】

$$M := \begin{pmatrix} M_r \\ M_r^2 \\ \cdots \\ M_r^k \end{pmatrix} : a \mapsto \begin{pmatrix} b_1 \\ b_2 \\ \cdots \\ b_k \end{pmatrix} = \begin{pmatrix} \gamma^r \cdot a \\ \gamma^{2r} \cdot a \\ \cdots \\ \gamma^{kr} \cdot a \end{pmatrix} \quad (3-13)$$

## 【0066】

上記(3-13)に示すように、行列Mが、データaに対してγ<sup>r</sup>～γ<sup>kr</sup>倍演算(×γ<sup>r</sup>)をそれぞれ行うk個の演算を規定している。

## 【0067】

この場合には、図12に示すように、CPU34が、データFS0に対してγ<sup>r</sup>～γ<sup>kr</sup>倍演算(×γ<sup>r</sup>)をそれぞれ行う演算回路21<sub>1</sub>～21<sub>k</sub>を有する演算回路11の構成を示す構成データを生成する。

## 【0068】

以上説明したように、本実施形態の回路構成方法では、上述したように図8に示すステップST13において、複数の第1の演算(D倍演算、α倍演算)を構成する複数の第2の演算のうち、同じデータに対して同じ演算を行う上記第2の

演算を特定する。

そして、ステップST14において、上記複数の第1の演算で共用され上記特定された上記第2の演算を行う第1の演算回路と、上記複数の第1の演算のそれを構成する上記複数の第2の演算のうち上記特定された上記第2の演算以外の演算を行う第2の演算回路とからなる演算回路11，11aを構成する。

そのため、本実施形態の回路構成方法によれば、演算回路11，11aを小規模に構成できる。

### 【0069】

また、本実施形態の回路構成方法では、図8に示すステップST12で、ステップST11で入力した上記（3-7）に示す演算回路11が行う複数の演算のそれについて、上記所定の回数に対応する数の第1の線形変換Dを合成して得られる第2の線形変換（第1の演算）を行う上記（3-9）に示す行列Mを生成し、これに対して上述したステップST13，ST14の処理を行う。

そのため、本実施形態の回路構成方法によれば、演算回路11，11aを小規模に構成できると共に、演算時間を短縮できる。

また、本実施形態の回路構成方法では、図9および図11に示すように、演算回路11が、データFS0に対して、第1の演算を並列に行うため、演算時間をさらに短縮できる。

すなわち、演算回路211～21kにおいてデータFS0（データa）を並列に処理するため、データb1～bk（データOUT1～OUTk）の全てを略同じタイミングで得ることができる。

そのため、データFS0を入力してからデータb2～bkを得るまでの時間を図3に示す構成に比べて短縮した演算回路11を構成（設計）できる。

### 【0070】

#### 〔第2実施形態〕

本実施形態では、有限体F（2<sup>4</sup>）上の元として扱われる4ビットのデータD（=D[3], D[2], D[1], D[0]）を縦ベクトルと見なし、当該データDに対して下記（3-14），（3-15）で示す行列M1, M2で示される2つの線形変換を施す回路を構成する場合を例示する。

【0071】

【数29】

$$M1 = \begin{pmatrix} 1 & 1 & 0 & 1 \\ 1 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 1 & 1 & 0 \end{pmatrix} \quad (3-14)$$

【0072】

【数30】

$$M2 = \begin{pmatrix} 0 & 1 & 0 & 1 \\ 1 & 0 & 1 & 1 \\ 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \end{pmatrix} \quad (3-15)$$

【0073】

従来では、出力値  $E1 = M1 \cdot D$ 、  $E2 = M2 \cdot D$  は、それぞれ縦ベクトルとして表現され、下記 (3-16)、(3-17) で示される。

【0074】

【数31】

$$\begin{aligned} E1 &= (E1[3], E1[2], E1[1], E1[0]) \\ &= (D[1]+D[2], D[3], D[0]+D[2], D[0]+D[1]+D[3]) \end{aligned} \quad (3-16)$$

【0075】

【数32】

$$\begin{aligned} E2 &= (E2[3], E2[2], E2[1], E2[0]) \\ &= (D[1], D[0], D[0]+D[2]+D[3], D[1]+D[2]) \end{aligned} \quad (3-17)$$

【0076】

従来の回路構成方法では、図13に示すように、上記 (3-16) に示す演算を行う演算回路402と、上記 (3-17) に示す演算を行う演算回路403とを有する演算回路401が構成される。

演算回路402は、加算回路411、412、413、414で構成される。

また、演算回路403は、加算回路421、422、423で構成される。

【0077】

本実施形態の回路構成方法は、上記 (3-14)、(3-15) に示す行列M

1, M2 によって表現される線形変換を, 有限体F (2<sup>4</sup>) 上の元として扱われる4ビットのデータD (=D [3], D [2], D [1], D [0]) に施すことは同じである。

本実施形態では、2つの4×4行列を用いる代わりに、行列M1とM2とを連結した下記(3-18)に示される行列Mを用いる。

【0078】

【数33】

$$M = \begin{pmatrix} M1 \\ M2 \end{pmatrix} = \begin{pmatrix} 1 & 1 & 0 & 1 \\ 1 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 1 & 1 & 0 \\ 0 & 1 & 1 & 0 \\ 1 & 0 & 1 & 1 \\ 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \end{pmatrix} \quad (3-18)$$

【0079】

本実施形態の回路構成方法では、上記行列Mの演算を行い、上記(3-16), (3-17)内の演算において、行列M1に相当する第1の演算と行列M2に相当する第1の演算とを構成する複数の第2の演算のうち、共通する第2の演算である「D [0] + D [2]」、並びに「D [1] + D [2]」を特定する。

そして、図14に示すように、第2の演算「D [0] + D [2]」を行う図13に示す加算回路412と421と、第2の演算「D [1] + D [2]」を行う図13に示す加算回路413と422が共用化され、加算回路412, 413が削減され、図13に示す演算回路401に比べて、回路規模が縮小された演算回路403が構成される。

これにより、図13に示す演算回路401と同じ演算を行う図14に示す演算回路403を、演算回路401に比べて小規模に構成できる。

【0080】

本発明は上述した実施形態には限定されない。

その他の実施形態として、上記所定の基底として下記(3-19)に示す基底を用い、上記データaを下記(3-20)のように示し、前記データaをm次元

ベクトルとして下記（3-21）のように示してもよい。

【0081】

【数34】

$$\{1, \gamma, \gamma^2, \dots, \gamma^{m-1}\} \quad (3-19)$$

【0082】

【数35】

$$a = a_0 + a_1 \gamma + a_2 \gamma^2 + a_3 \gamma^3 + \dots + a_{m-1} \gamma^{m-1} \quad (3-20)$$

【0083】

【数36】

$$a = \begin{pmatrix} a_0 \\ a_1 \\ a_2 \\ \vdots \\ \vdots \\ a_{m-1} \end{pmatrix} \quad (3-21)$$

【0084】

【発明の効果】

以上説明したように、本発明によれば、所定データに対してそれぞれ異なる複数の演算を行なう演算回路を構成する場合に、当該演算回路を小規模に構成できる回路構成方法、その装置およびそのプログラムを提供することができる。

【図面の簡単な説明】

【図1】

図1は、本発明の関連技術を説明するための図である。

【図2】

図2は、本発明の関連技術を説明するための図である。

【図3】

図3は、本発明の関連技術を説明するための図である。

【図4】

図4は、本発明の関連技術を説明するための図である。

【図5】

図5は、本発明の関連技術を説明するための図である。

【図6】

図6は、本発明の第1実施形態の回路構成方法で構成（設計）される演算回路の周辺回路を説明するための図である。

【図7】

図7は、本発明の第1実施形態の回路構成方法を実行するコンピュータを説明するための図である。

【図8】

図8は、本発明の第1実施形態の回路構成方法の手順によって演算回路を構成する場合を説明するためのフローチャートである。

【図9】

図9は、本発明の第1実施形態の回路構成方法で構成（設計）される演算回路を説明するための図である。

【図10】

図10は、図9に示す演算回路のデータ出力タイミングを説明するための図である。

【図11】

図11は、図9に示す演算回路の具体例を説明するための図である。

【図12】

図12は、本発明の第1実施形態の回路構成方法によって構成される $\gamma^r \sim r$ 倍演算 $(\times \gamma^r)$ を行う演算回路を説明するための図である。

【図13】

図13は、本発明の第2実施形態の回路構成方法の関連技術を説明するための図である。

【図14】

図14は、本発明の第2実施形態の回路構成方法を説明するための図である。

【符号の説明】

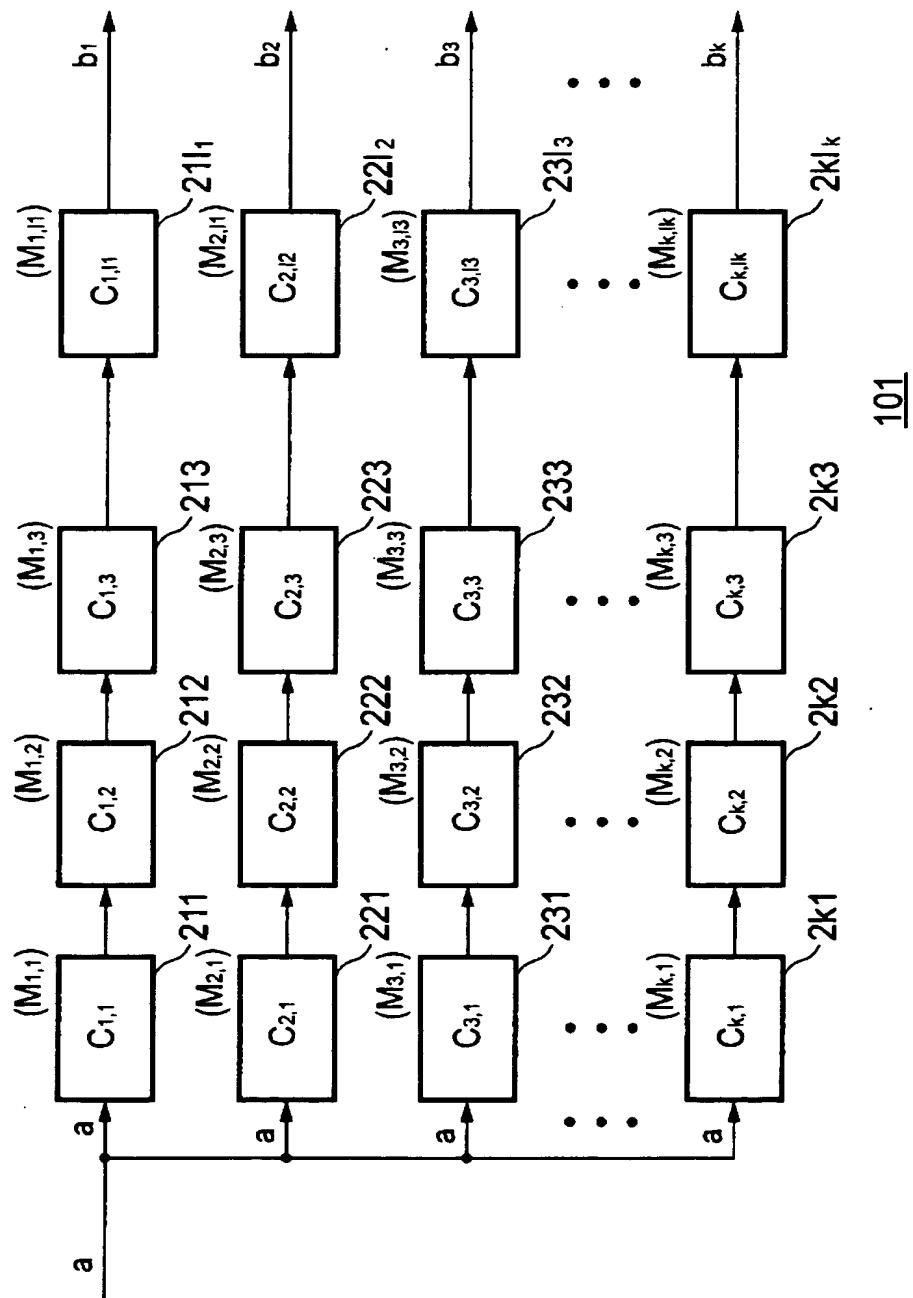
1 1 … 演算回路、 1 2 … セレクタ、 1 3<sub>0</sub> ~ 1 3<sub>k</sub> … レジスタ、 1 4 … 演算回路、 2 1<sub>1</sub> ~ 2 1<sub>k</sub> … 演算回路、 3 0 … バス、 3 1 … 操作部、 3 2 … ディスプレ

イ、33…メモリ、41…プログラム、42…データ

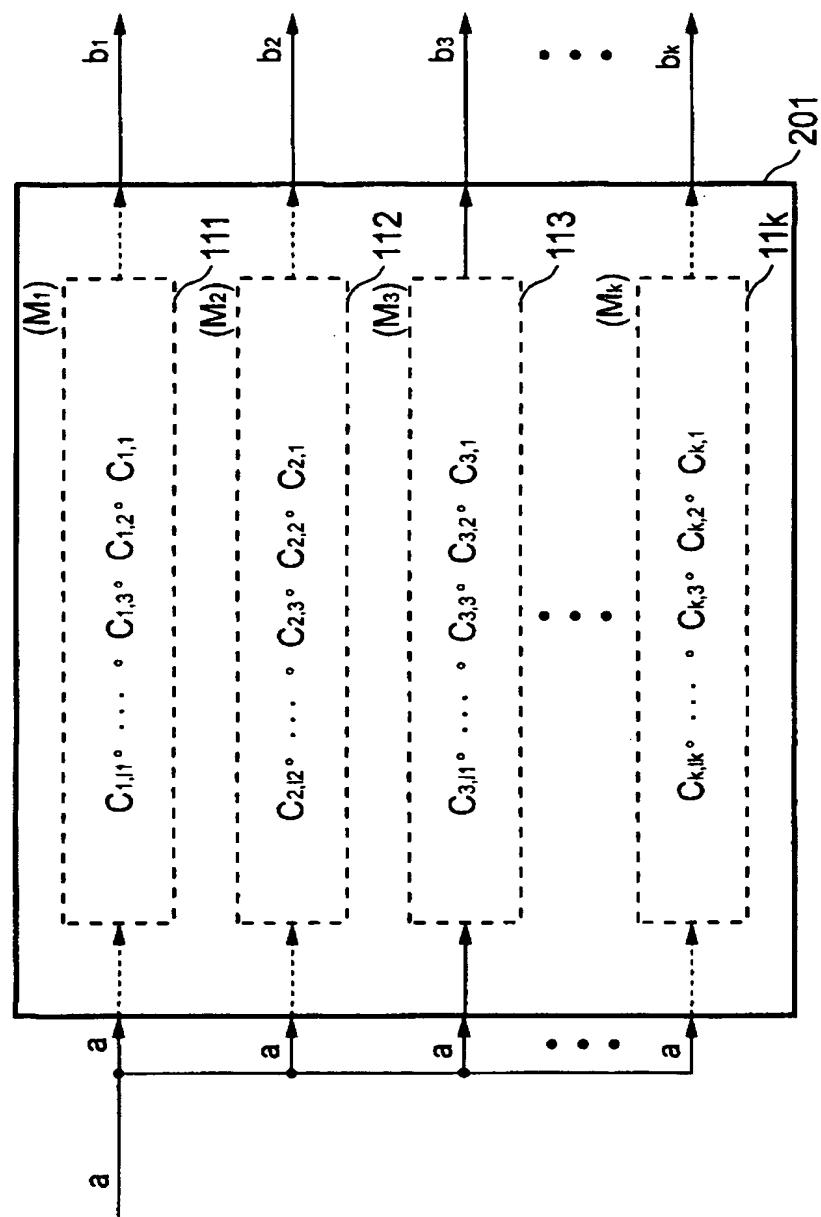
### 【書類名】

四面

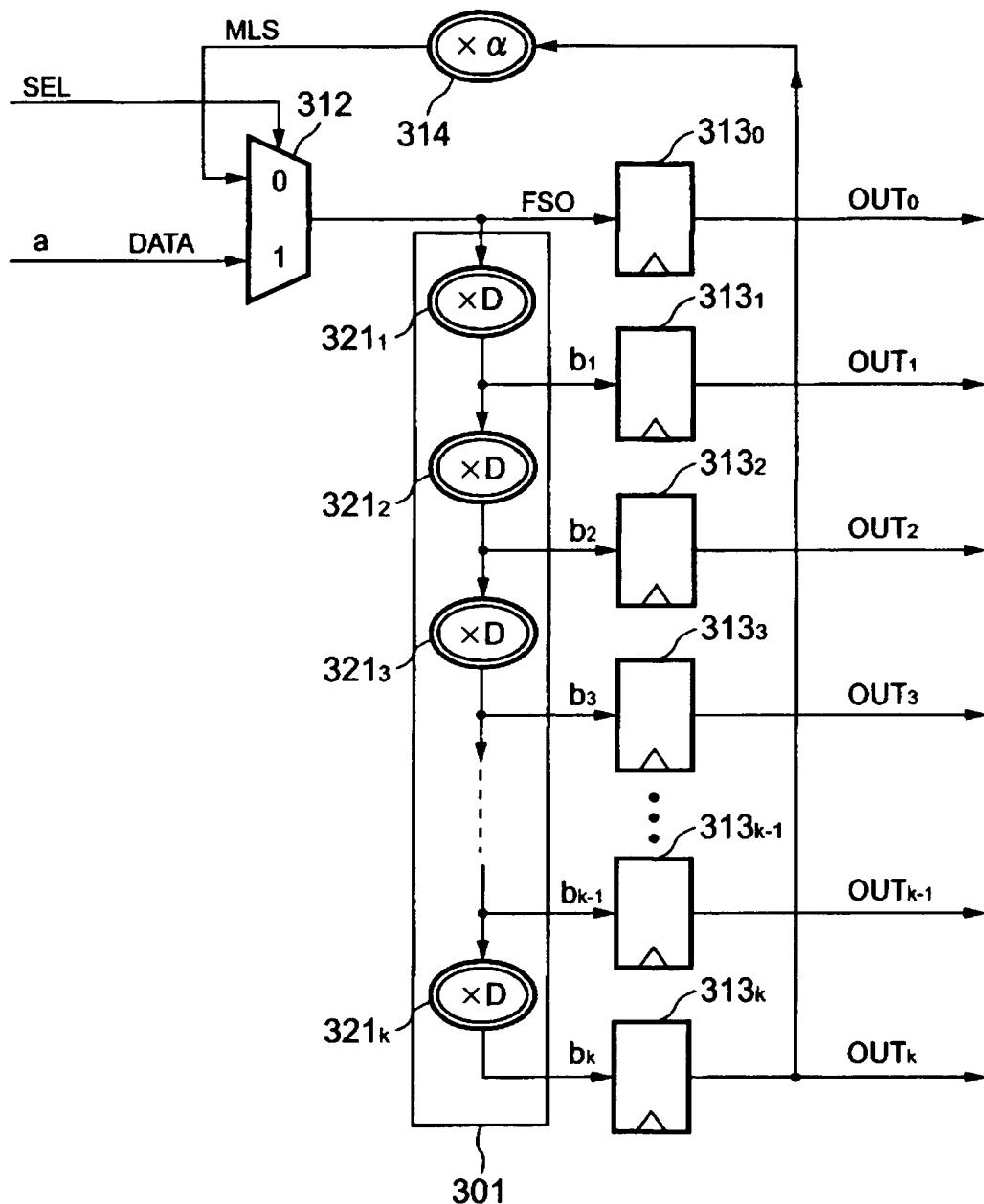
【圖 1】



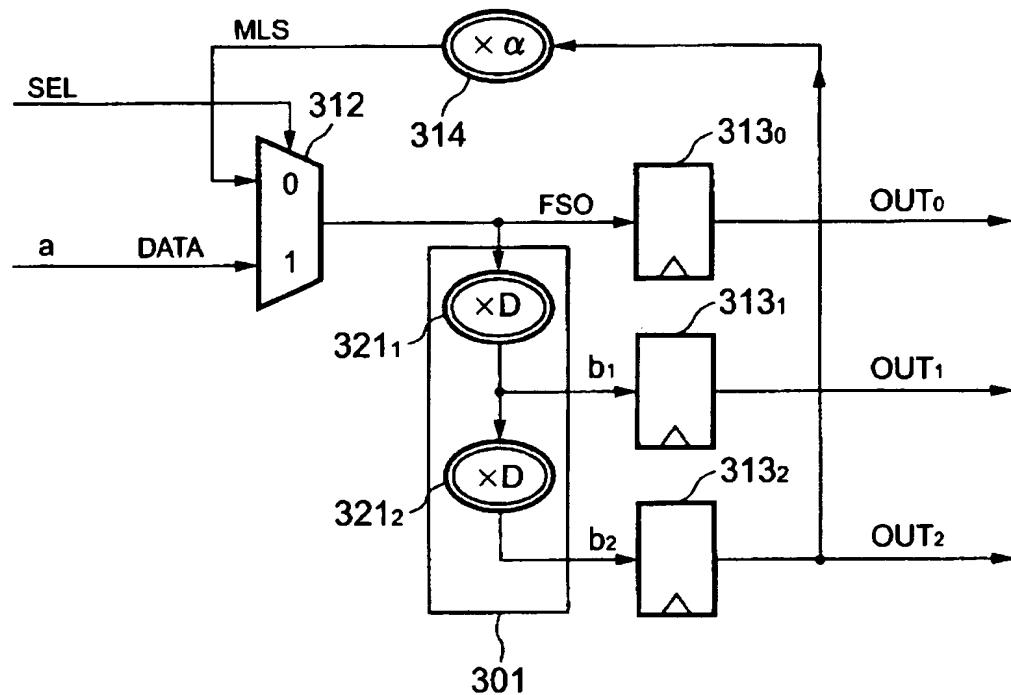
【図2】



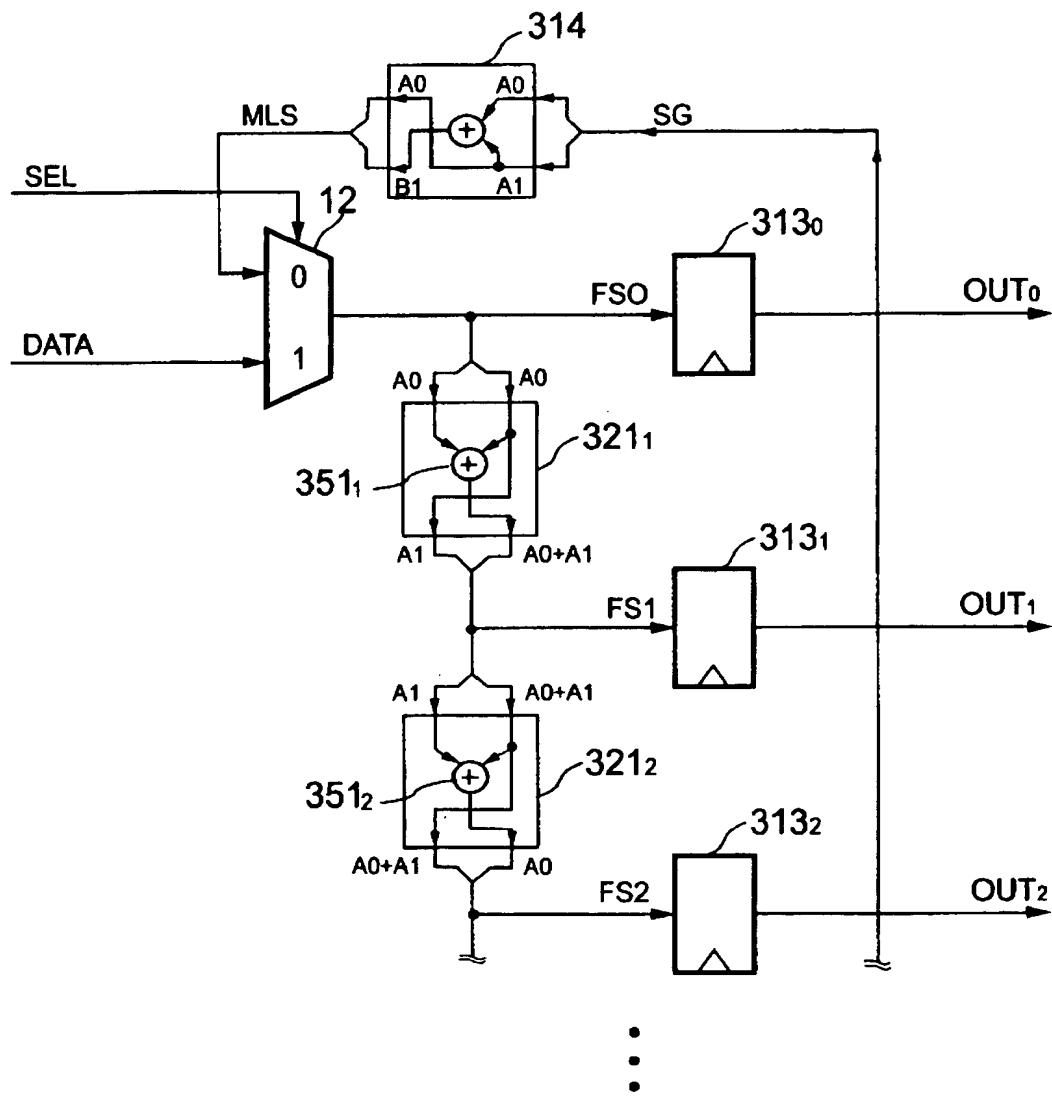
【図3】



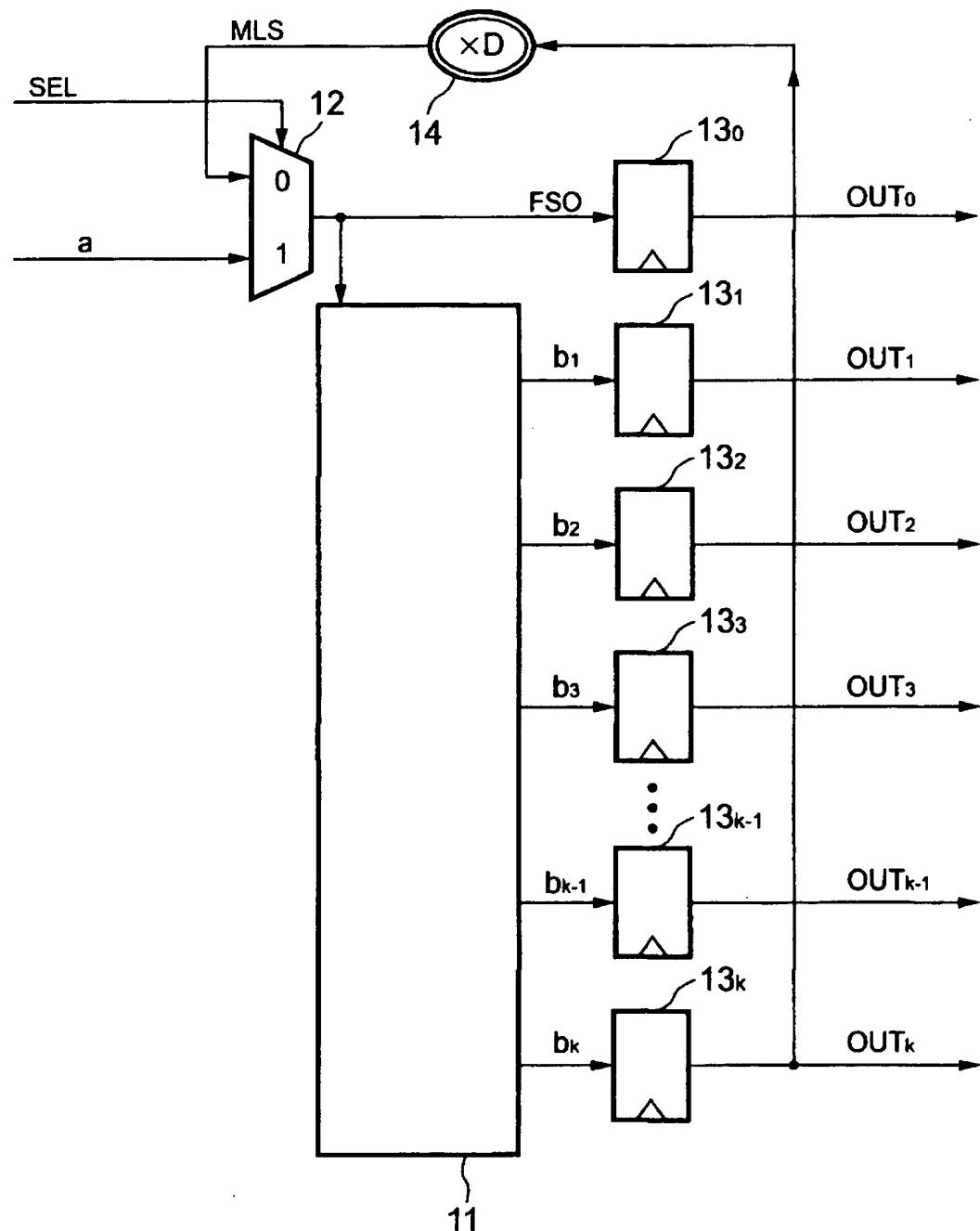
【図4】



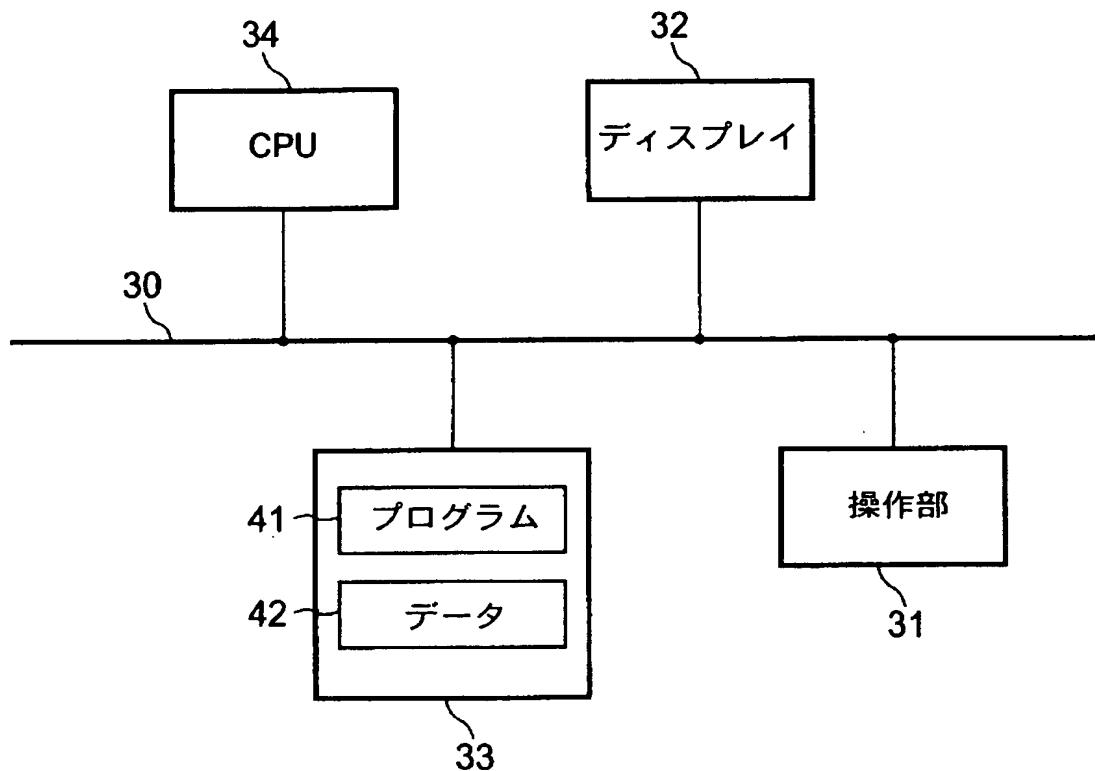
【図5】



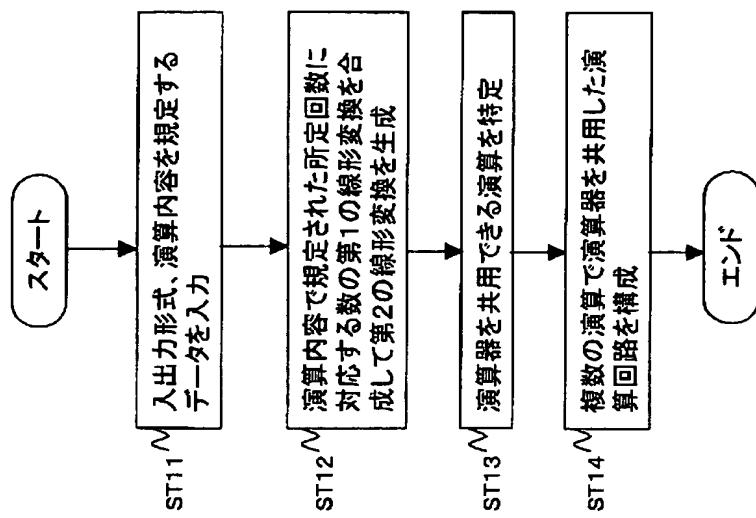
【図 6】



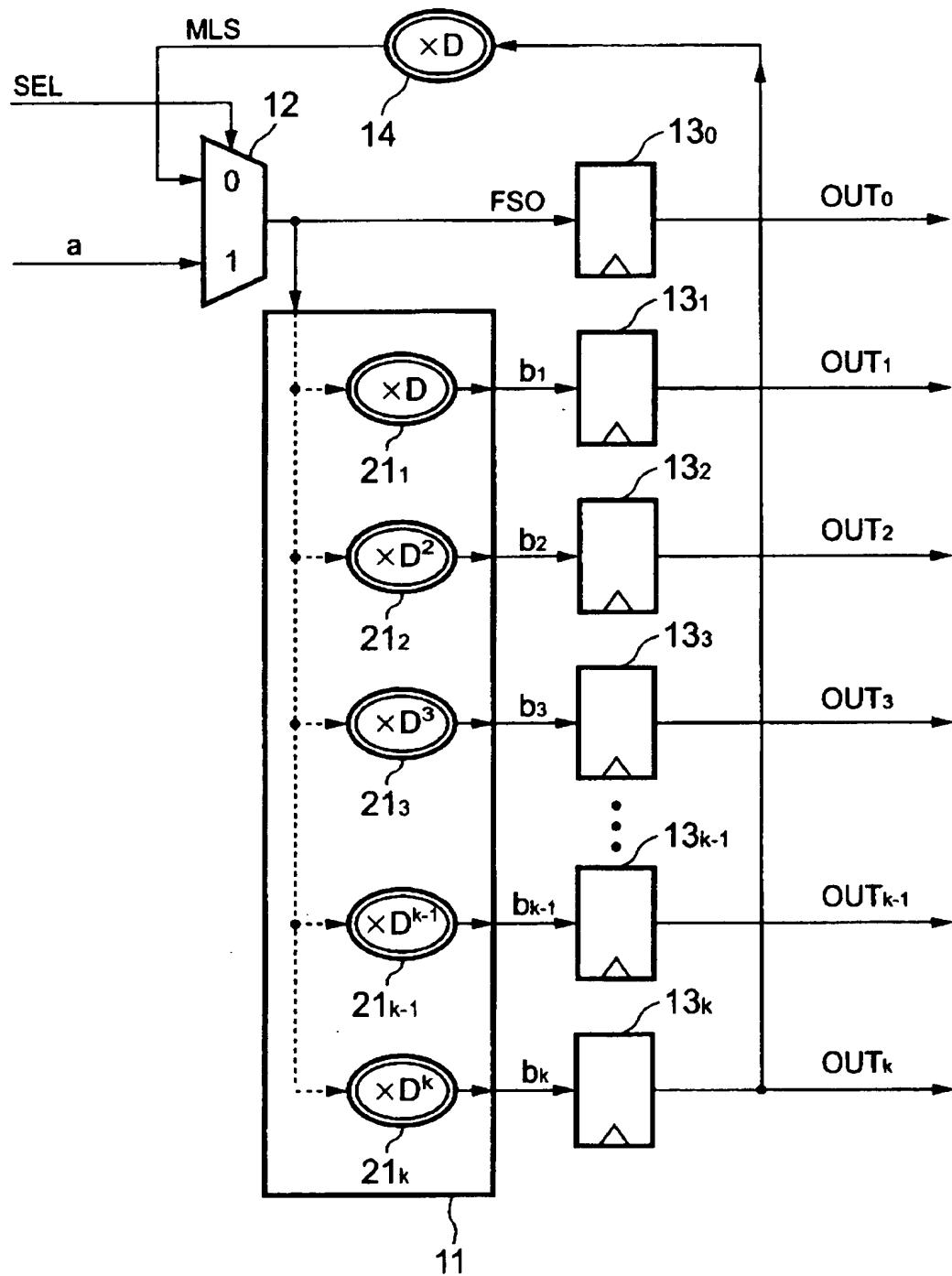
【図7】



【図 8】



【図9】

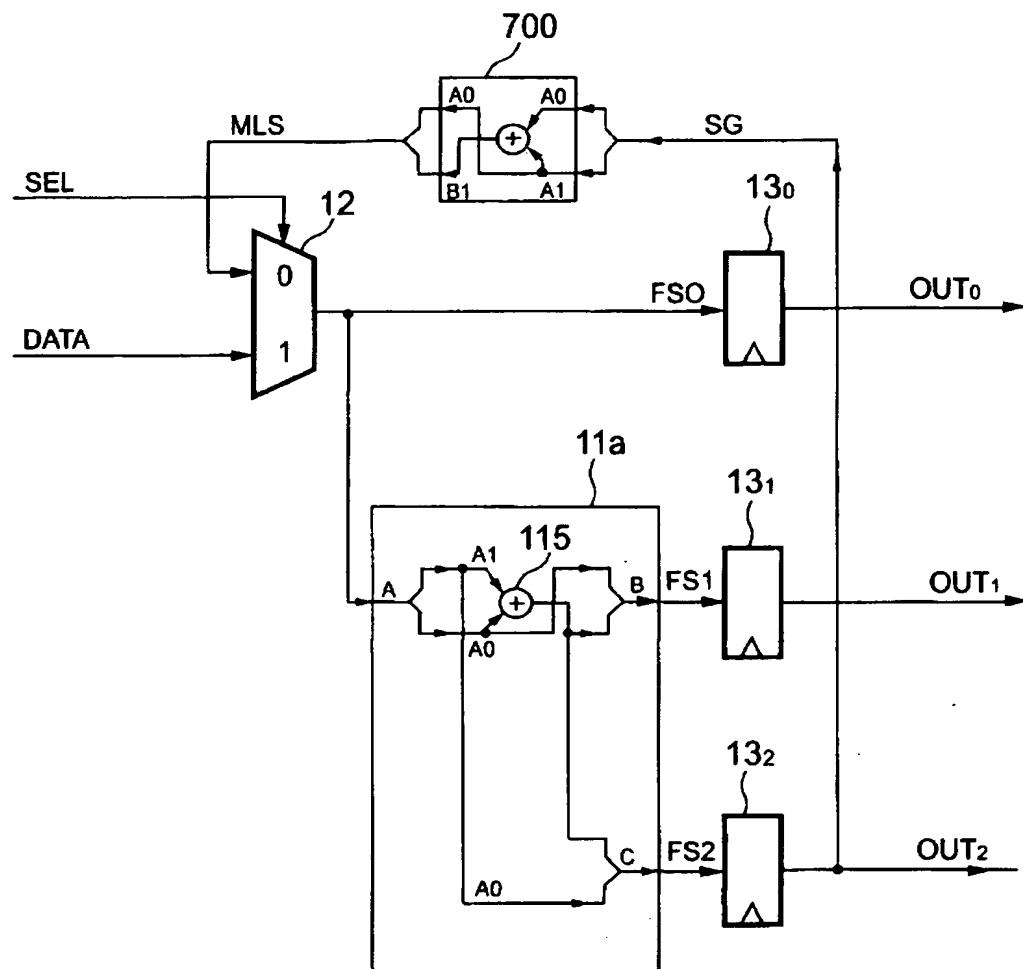


【図10】

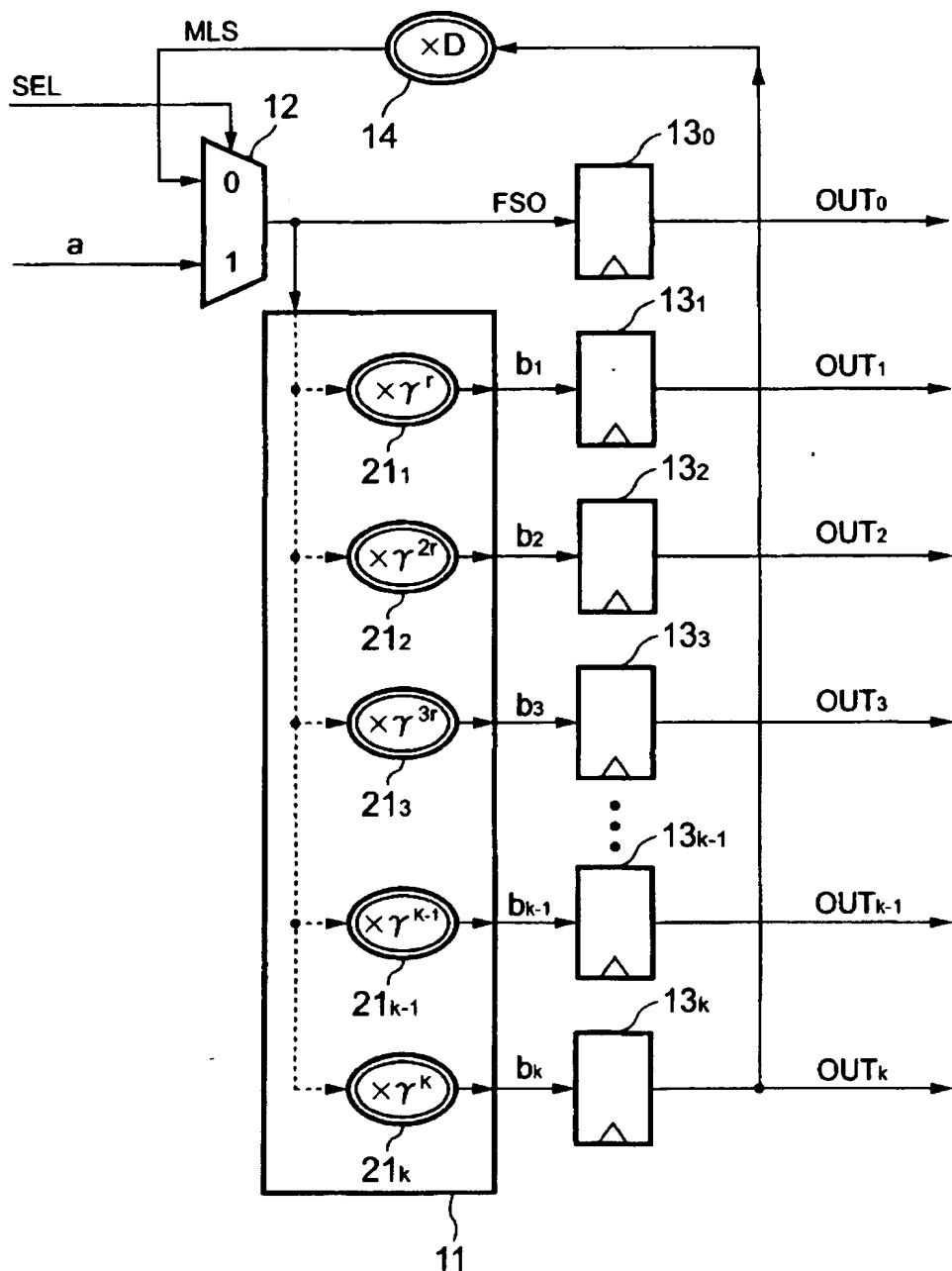
OUT <sub>0</sub> :	a	D <sup>K+1</sup> a	D <sup>2K+2</sup>	• • •
OUT <sub>1</sub> :	Da	D <sup>K+2</sup> a	D <sup>2K+3</sup>	• • •
OUT <sub>2</sub> :	D <sup>2</sup> a	D <sup>K+3</sup> a	D <sup>2K+4</sup>	• • •
OUT <sub>3</sub> :	D <sup>3</sup> a	D <sup>K+4</sup> a	D <sup>2K+5</sup>	• • •
⋮	⋮	⋮	⋮	⋮
OUT <sub>k</sub> :	D <sup>k</sup> a	D <sup>K+K+1</sup> a	D <sup>3K+1</sup>	• • •

→ 時間

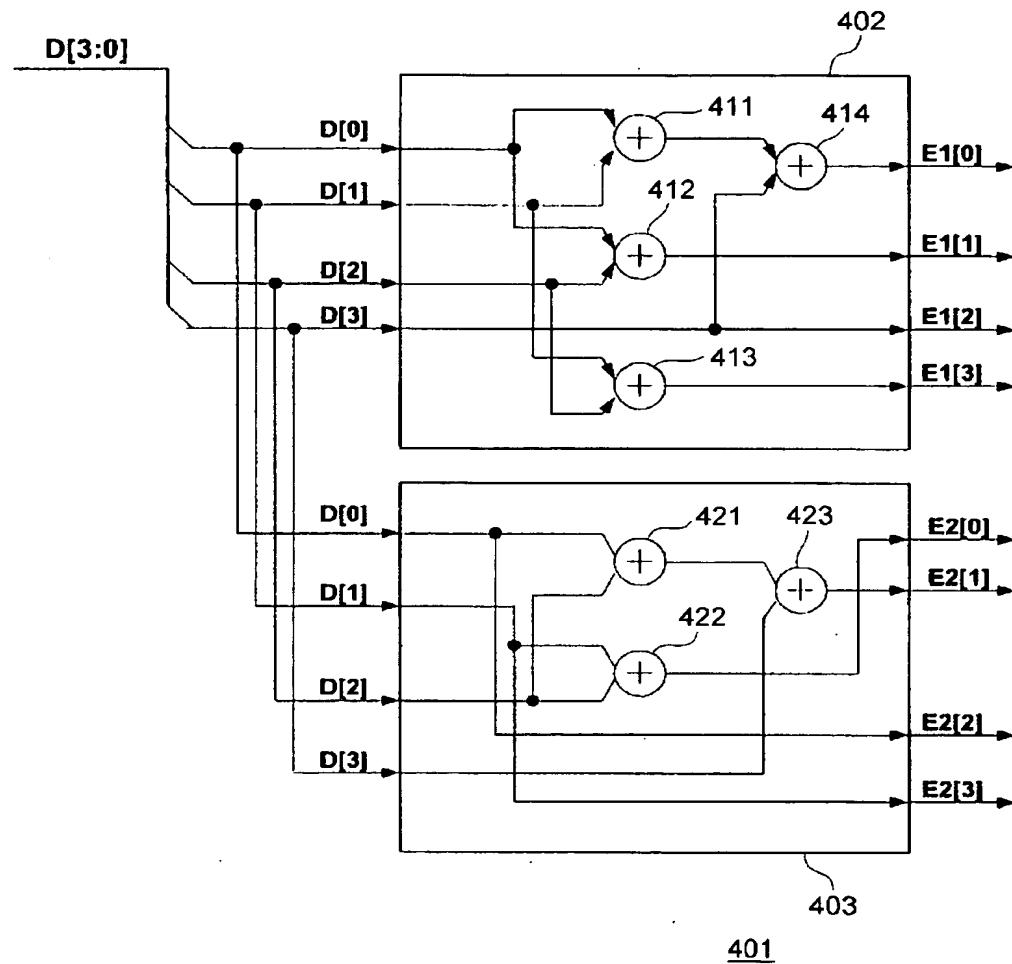
【図11】



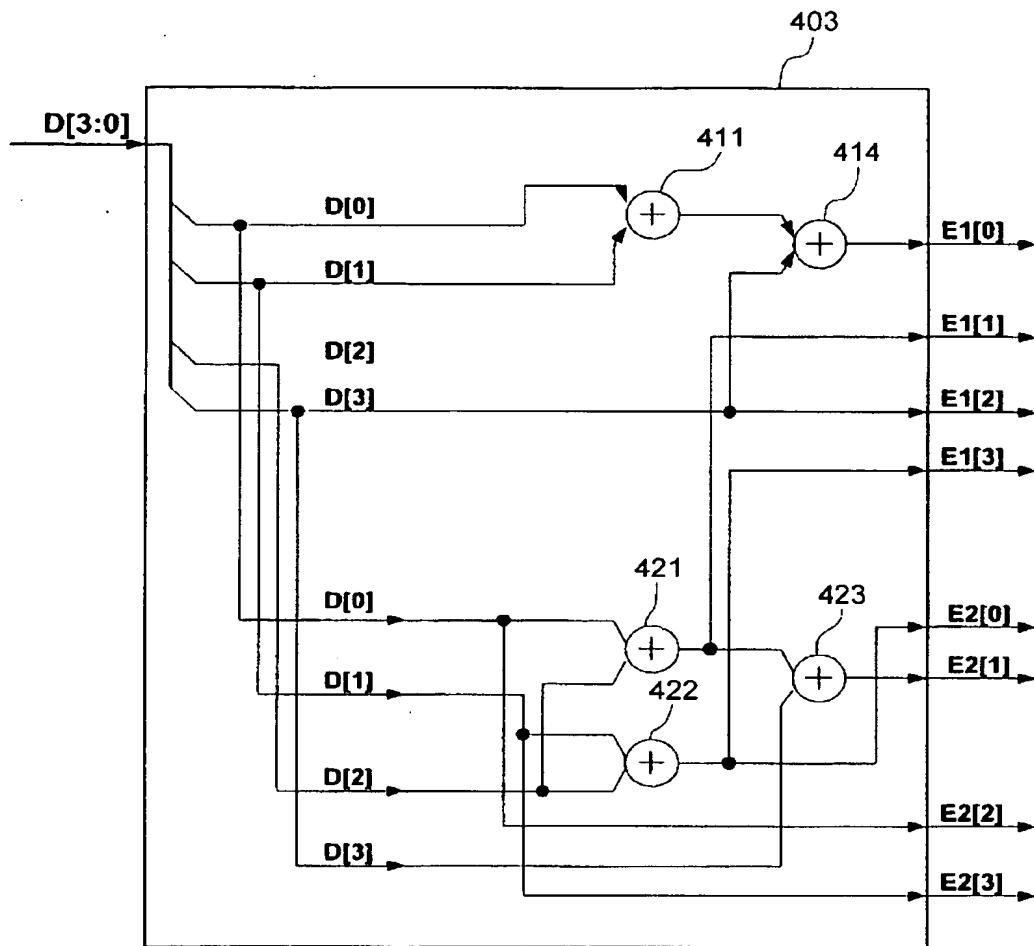
【図12】



【図13】

401

【図14】



【書類名】 要約書

【要約】

【課題】 所定データに対してそれぞれ異なる複数の演算を行なう演算回路を構成する場合に、当該演算回路を小規模に構成できる回路構成方法を提供する。

【解決手段】 所定のデータに対してそれぞれ異なる複数の第1の演算を施す演算回路を設計する場合に、複数の第1の演算のそれぞれを構成する複数の第2の演算のうち、同じデータに対して同じ演算を行う前記第2の演算を特定する（S T 1 3）。そして、複数の第1の演算で共用され S T 1 3 で特定された第2の演算を行う演算回路を有する演算回路を構成する（T 1 4）。

【選択図】 図8

特願2002-331677

出願人履歴情報

識別番号 [000002185]

1. 変更年月日 1990年 8月30日

[変更理由] 新規登録

住所 東京都品川区北品川6丁目7番35号  
氏名 ソニー株式会社